REMARKS

Applicants have now had an opportunity to carefully consider the Examiner's comments set forth in the Office Action of July 2, 2007.

Reconsideration of the Application is requested.

The Office Action

Claims 1-3, 9-10 and 13-27 are pending in the application.

Claims 1-3, 5, 6, 8-10 and 13-27 stand rejected under 35 U.S.C. §102 as being anticipated by Schultz (U.S. patent No. 6,948,094).

Claims 4-8, 11 and 12 have been cancelled.

Telephonic Interview with the Examiner

Applicants gratefully acknowledge the opportunity given by the Examiner to discuss the present application in a number of telephonic interviews. The Examiner and Applicants discussed the present application and cited prior art. As a result of the interview, it is the Applicants' understanding that the amended claims overcome the 102 rejection over cited prior art.

Amendments to the Drawings

Applicants submit a replacement drawing sheet containing an amended Figure 2.

Figure 2 has been amended to include a block 220. The support for this amendment may be found in specification in paragraphs 23 and 29, for example.

Figure 2 has been further amended to replace the text "no, error consumed" with "no" and the text "yes, error not consumed" with "yes."

Figure 2 has been further amended to replace text "DP set?" in block 206 with "DP Flag Set?".

It is respectfully requested that the original drawing sheet containing Figure 2 be replaced with the replacement drawing sheet.

Amendments to Specification

The specification has been amended to correct typographical mistakes. It is respectfully submitted that amendments to specification do not represent any new subject matter.

Claims Distinguish over Cited Prior Art

Claim 1 calls for, among other elements:

pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events by a user;

error-checking a unit of data by an error-control decoder;

detecting an uncorrectable error in the unit of data by the error-control decoder;

if the uncorrectable error is detected in the unit of data, based on the pre-determined data poisoning policy, determining if the detected uncorrectable error is a data poisoning event;

marking the unit of data containing a data poisoning event with a software-visible bit by the error-control decoder which is a status bit to indicate to an operating system that the data unit contains the data poisoning event;

determining, based on the pre-determined data poisoning policy, if the unit of data containing the poisoning event is to be acted upon;

handing over the data units including the detected uncorrectable errors including data poisoning events from the error-control decoder to the operating system.

Schultz is directed to an error-recovery system in which the processor is placed into a suspended state. Processor independent instructions attempt to correct the error. Nowhere does Schultz describe or suggest a user defined software-programmable data poisoning policy.

The present Office Action equates the OS error handling policy, as described in Schultz, with the user defined software-programmable data poisoning policy. Schultz describes the OS error handling policy which is an OS-dependent, software based error handling policy that is consulted only after errors have been detected by the hardware and notification has been sent to the OS. This is entirely different from the software-programmable data poisoning policy according to the concepts of the present application. As claimed in claim 1, the software-programmable data poisoning policy is OS-independent, as it only needs to be programmed a user. Once the data poisoning policy has been predefined and programmed, it is used by the hardware directly, independent of the OS. When the error-control decoder detects an error, the software-programmable data-poisoning policy is consulted by the error-control decoder to determine how to handle the error, i.e. whether or not the error

requires data poisoning, and if so, what sort of notification to generate to the OS. Only after the software-programmable data poisoning policy has been used by the error-control decoder hardware does the error get handed off to the OS, with the proper software-visible bits already set by hardware. The OS may then handle the error in accordance with the software-visible bits set by the predefined programmable data poisoning policy, for example, using an OS error-handling policy if one is available. Thus, Schultz does not disclose or suggest the software-programmable data poisoning policy which is independent from the OS error handling policy and controls actions of the OS error handling policy.

Further, Schultz does not disclose or suggest the software-visible status bit as claimed in claim 1. The software-visible bit of claim 1 is a bit set by the error-control decoder hardware to indicate to the OS when the data unit contains a data poisoning event. This is different from the processor configuration bits of Schultz, which are control bits set by the processor to control the escalation of the error visible to the processor. Thus, Schultz does not disclose or suggest the software-visible status bit recited in claim 1.

It is therefore respectfully submitted that **claim 1 and dependent claims 2-3, 9-10, and 13** distinguish patentably and unobviously over Schultz.

Claim 14 calls for, among other elements: a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events. The arguments above regarding claim 1 are equally applicable here. It is therefore respectfully submitted that **claim 14 and dependent claims 15-20** distinguish patentably and unobviously over Schultz.

Claim 21 calls for, among other elements: pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events. The arguments above regarding **claim 1** are equally applicable here. It is therefore respectfully submitted that **claim 21 and dependent claims 22-23** distinguish patentably and unobviously over Schultz.

Claim 24 calls for, among other elements: pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events. The arguments above regarding claim 1 are equally applicable here. It is therefore respectfully submitted that **claim 24 and dependent claims 25-27** distinguish patentably and unobviously over Schultz.

CONCLUSION

For at least the reasons detailed above, it is submitted that all claims remaining in the application **(claims 1-3, 9-10 and 13-27)** are in condition for allowance. The foregoing comments do not require unnecessary additional search or examination.

The undersigned attorney of record hereby authorizes charging any necessary fees, other than the issue fee, to the Deposit Account No. 22-0261.

If the Examiner finds a personal contact advantageous to the disposition of this case, the Examiner is invited to call Marina Zalevsky, at telephone number 202-344-4975.

Respectfully submitted,

Date: October 2, 2007

James R. Burdett
Registration No. 31,594
Marina V. Zalevsky
Registration No. 53,825
VENABLE LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300

JRB:MVZ
#886163